KOREAN PATENT ABSTRACTS

(11)Publication number: 1019990088046 A

(43)Date of publication of application:

27.12.1999

(21)Application number: 1019990016020

(22)Date of filing: 04.05.1999

(30)Priority: 07.05.1998 1

(51)Int. Cl H04K 1/00

(71)Applicant: LUCENT TECHNOLOGIES INC.

(72)Inventor: BERENZWEIG ADAM L.

(54) METHOD AND AIF(AUTHENTICATION INTEROPERABILITY FUNCTION) IN A COMMUNICATION SYSTEM, ESPECIALLY FOR ENABLING A USER TO PERFORM LOAMING BETWEEN DIFFERENT AUTHENTICATION SYSTEMS

(57) Abstract:

PURPOSE: A method and AIF(Authentication Interoperability Function) in a communication system are provided to generate triplet from current SSD(Shared Secret Data) when loaming by a network based on triplet is performed and generate SSD from the triplet when the user performs loaming by SSD network, thereby enabling a user to simultaneously use both networks. CONSTITUTION: An AIF(Authentication Interoperability Function) in a communication system when a user is located in a second network having different authentication method with a first network comprises the following steps of: receiving challenge/response from Authentication data base of a first network; generating a second key from the challenge/response; and transmitting the second key to repeater of a second network for authenticating a user from the first network.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04K 1/00

(11) 공개번호 특1999-0033046
(43) 공개일자 1999년12월27일

(21) 출원번호 10-1999-0016820
(22) 출원일자 1999년05월04일
(30) 우선권주장 9/073,970 1998년05월07일 미국(US)
(71) 출원인 콴텔트 테크놀러지스 인크
미합중국 뉴저지 미라이 씨 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자 버넌조엘마그아달레
미국뉴욕주10603화이트플레12-001소로12번가70
(74) 대리인 김창세, 장성구

심사청구 : 없음

(54) 통신시스템에서의인증와동화신호방법

요약

본 발명은 상이한 인증(authentication) 기법을 사용하는 두 개의 통신 네트워크 간의 로밍(global roaming)을 가능케 하는 방법 및 장치에 관한 것이다. 인증 연동 동션(authentication interoperability function : AIF) 및 방법들, 여러개의 트리플릿 기반 네트워크(triplet-based network)와 공유 비밀 데이터(shared secret data : SSD) 네트워크와 같은 상호의 네트워크의 인증 기법을 가능 동케한다. 실질적으로 SSD 인증을 사용하는 네트워크의 사용자가 트리플릿 기반 네트워크로 로밍할 경, 인증 연동 동션은 현재의 SSD로부터 트리플릿을 생성한다. 트리플릿 사용자가 SSD 네트워크로 로밍할 때 AIF는 트리플릿으로부터 SSD를 생성한다.

대표도

도3

명세서

도면의 간단한 설명

도 1은 종래 기술에 따른 GSM 네트워크의 기본 구성 요소를 도시한 블록도,

도 2는 종래 기술에 따른 GSM 네트워크에서 전송되는 메시지를 도시한 도면,

도 3a 및 3b는 종래 기술에 따른 IS-41 네트워크의 기본 구성 요소를 도시한 블록도,

도 4는 도 3에 도시된 종래 기술에 따른 IS-41 네트워크에서 전송되는 메시지를 도시한 도면,

도 5는 일반적인 통신 시스템의 블록도,

도 6은 일반적인 이동 통신 시스템의 블록도,

도 7은 IS-41 사용자가 GSM 네트워크로 로밍(roaming)하는 방법을 도시한 블록도,

도 8은 GSM 사용자가 IS-41 네트워크로 로밍하는 방법을 도시한 도면,

도 9는 로밍하는 IS-41 사용자를 도시한 상세도,

도 10은 로밍하는 GSM 사용자를 도시한 상세도,

도 11은 일반적인 네트워크 인터페이스를 도시한 도면.

도면의 주요 부분에 대한 부호의 설명

218 : 제 1 네트워크 220 : 제 2 네트워크

222 : 네트워크 대 네트워크 인터페이스(NNI)

302, 305 : 홈 위치 레지스터 304, 308 : 방문 위치 레지스터

310 : 이동 단말기(MT)　　　312 : UIM

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 통신 시스템에서의 사용자의 인증에 관한 것으로, 특히, 사용자가 상이한 인증 기법을 구현하는 두 개의 통신 시스템 사이를 로밍하는 경우에 무선 네트워크에서의 사용자의 인증에 관한 것이다.

현재 미국, 유럽, 일본에서는 상이한 통신 표준을 사용하고 있다. 미국은 현재 표준을 관리하는 세 개의 주 시스템을 사용하고 있다. 첫 번째 시스템은 시분할 다중 액세스 시스템(time division multiple access system : TDMA)으로 IS-136에 의해 통제되고, 두 번째 시스템은 IS-95에 의해 통제되는 코드(code) 분할 다중 액세스(CDMA) 시스템이며, 세 번째는 고성능 이동 전화 시스템(advanced mobile phone system : AMPS)이다. 세 가지 통신 시스템 모두는 시스템간 신호 전달을 위해 IS-41 표준을 사용하는데, IS-41 표준은 인증 절차를 정의하고 있다.

TDMA에서, 사용자들은 주파수 대역을 공유하고, 사용자들을 구별하기 위해 제어된 시간 슬롯을 사용하여 각각의 사용자의 음성을 저장하고 압축하여 빠른 패킷으로서 전송하기 때문에 "시분할"이라 명명된다. 수신기에서 패킷은 압축 해제된다. IS-136 프로토콜에서는 세 명의 사용자가 주어진 채널을 공유한다.

통상적인 시스템은 각각 단일 신호를 이따금 간헐적으로 협대역 상에서 전송한다. 대조적으로, CDMA는 변대로 동작하여, 약하지만 매우 넓은 대역의 신호를 전달한다. 고유의 코드는 스펙트럼의 넓은 영역에 걸쳐 신호를 "확산시키고(spread)"(따라서, 다른 이름으로는 확산 스펙트럼이라 함), 수신기는 동일한 코드를 사용하여 잡음으로부터 신호를 복원한다. 절대적으로 낮은 전력의 신호라 하더라도 이러한 코드는 매우 강하고 안전한 채널이 형성될 수 있으며, 신호가 잡음층(noise floor)보다 약할 수 있다. 더욱이, 상이한 코드를 사용함으로써 다수의 상이한 채널이 상호 간섭하지 않으면서도 동시에 동일한 스펙트럼을 공유할 수 있다.

AMPS 시스템은 아날로그 시스템이다.

유럽은 유럽 원격 통신 표준 연구소(European Telecommunications Standard Institute : ETSI)에 의해 규정된 바와 같이 GSM(Global System for Mobiles) 네트워크를 사용한다. 이것은 유럽 외의 나라를 포함해서 세계 여러 국가에서 다수의 오퍼레이터(operator)가 GSM을 지원하고 있다. GSM은 TDMA 표준으로서 채널당 8명의 사용자를 가지고 있다. 20 msec 정도의 단위로 음성을 취하고, 압축하여 전송한다.

GSM은 900 MHz 캐리어 상에서 전송된다. 추가적인 용량을 제공하고 1.8 GHz(DCS 1800)로 동작하는 대체 시스템이 존재하는데, 이는 셀룰러 시스템(cellular system)보다 개인 통신 시스템(personal communication system : PCS)에서 더 자주 볼 수 있다. 동시에 일반으로, 미국도 1.9 GHz의 상이한 캐리어 상에서 동작하는 다른 GSM 시스템인 DCS-1900을 구현해 왔다.

일본의 표준은 이전에는 JDC(Japanese Digital Cellular)로 알려져 있던 개인 디지털 셀룰러(personal digital cellular : PDC)이다. 미국의 IS-54 프로토콜과 유사한 TDMA 표준인 PDC는 다른 나라에서는 사용되지 않고 있다.

GSM 네트워크는 가입자가 소유한 신용카드 크기의 카드인 사용자 식별 모듈(user identification module : UIM)을 사용하고, 가입자는 UIM을 임의의 GSM 송수화기에 넣어 넣어 임의의 GSM 송수화기를 "그들의" 전화로 변환시킨다. 이에 따라 그들의 고유 전화 번호가 다이얼링(dialing)될 때에 울리고, 호출에 대한 비용은 그들의 계좌로 청구될 것이고, 모든 선택 사항과 서비스가 접속되고, 음성 메일이 연결될 수 있는 등이 가능해진다. 상이한 UIM을 가진 사람들은 하나의 "물리적인(physical)" 송수화기를 공유할 수 있으며, 공유되는 하나의 송수화기는 UIM 당 하나씩해서 여러 개의 "가상(virtual)" 송수화기로 전환된다.

미국의 시스템과 유사하게, 전화(또는 UIM)가 이동함에 따라 GSM 네트워크도 "로밍"을 가능케 하므로, 상이한 네트워크 오퍼레이터들이 다른 네트워크들로부터의 가입자들을 인식하는(또한 받아들이는) 것에 동의한다. 따라서, 영국 가입자들이 프랑스 혹은 독일을 통해 이동할 수 있고며, 미국 사업가가 미국 시스템 등의 임의의 한 시스템 내에서 보스톤, 마이애미 혹은 시애틀에서 전화를 사용할 수 있는 것만큼이나 쉽게 그들의 GSM 전화를 사용하여 (그들의 영국 번호로) 호출하거나 호출을 수신한다.

가입자가 호출할 때는 전화 통신 시스템과 상관없이, 가입자의 전화는 요금 청구의 목적으로 서비스 제공자에게 호출자의 정체(identity)를 알려준다. 따라서, 서비스 제공자는 가입자가 허가된 사용자라는 것을 보증하기 위해 호출자의 정체를 "인증(authenticate)"해야 한다.

도 1 및 2는 종래 기술에 따른 GSM 인증 기법을 도시하고 있다. 이러한 인증 기법은 홈 위치 레지스터(home location register : HLR)(10), 방문 위치 레지스터(visiting location register : VLR)(20), UIM(32)을 구비하는 이동 단말기(mobile terminal : MT)(30)을 포함한다. 이동 단말기(30)가 호출하면, 리퀘스트(request)가 홈 위치 레지스터(10)에 전달되고 레지스터(10)는 루트 키(root key) K로부터 인증 트리플릿(authentication triplet)(RAND, SRES, K_c)을 생성한다. 트리플릿은 난수(random number) RAND, 서명 응답(signed response) SRES, 세션 키(session key) K_c를 포함한다. 트리플릿은 방문 위치 레지스터(20)에 제공되고, 레지스터(20)는 이동 단말기(30)에 난수 RAND를 전달한다. UIM(32)은 난수 RAND를 수신하고, 루트 키 K, 난수 RAND, 알고리즘 A3를 이용하여 서명 응답 SRES를 계산한다. 또한 UIM(32)는 루트

키 K는 난수 RAND, 등고리즘 A3을 이용하여 세션 키 K를 계산한다.

마찬가지로 과정 세션일 SRES는 이동 단말기(30)를 사용하는 가입자를 인증하기 위해 방문 위치 레지스터(20)로 리턴(return)되며 홈 위치 레지스터(10)로부터 수신된 SRES와 비교된다.

GSM "챌린지/응답(challenge/response)" 인증 시스템에서는, 방문 위치 레지스터(20)는 MIN(32) 및 홈 위치 레지스터(10)에 의해 홀딩(holding)되는 무작위 키 K로 결코 수신하지 않는다. 또한, VLR(20)은 MLR(10) 및 IMSI(32)에 사용된 인증 알고리즘을 알 필요가 없다. 또한, GSM 인증 기법에서, 트라블러는 홈 위치 레지스터(10)에 의해 알은 개별 호출에 연결된다. RAND는 128 비트이고, SRES는 32 비트이고, K는 64 비트로서, 통상적 데이터 모드(mod)인 라지오 리퀘스트에 대해 224 바이 데이터가 된다.

도 3a, 3b, 4는 미국의 TDMA, CDMA, AMPS 시스템에 사용된 몇몇 기술에 따른 IS-41 인증 기법을 도시하고 있다. 이 인증 기법은 홈 위치 레지스터(HLR)(60), 방문 위치 레지스터(VLR)(50), UIM 인터페이스 기능 단말기(MT)(56)를 포함하고 있다. A Key로 알려진 무등 키는 HLR(40) 및 UIM(62)에만 저장된다. 또한 비밀 데이터 SSD로 알려진 2개 키가 존재하고 이는 모든 동안에 VLR(50)에 전달된다. 도 3a에 도시된 바와 같이, SSD는 임포함 알고리즘을 사용해서 A key 및 랜덤 시드(random seed) RANDSSD로부터 생성된다. IS-41 네트워크에서, 이 알고리즘은 CAVE(Cellular Authentication and Voice Encryption)이다. MT(60)가 방문 네트워크로 진입할 때, VLR(50)은 HLR(40)에 인증 리퀘스트를 전달한다. HLR(40)은 하당 가입자의 SSD를 검색하고 두에 따른다.

일단 VLR(50)이 SSD를 갖게 되면, 도 3a와 도시한 바와 같이, HLR(50)은 HLR(40)에 상응하여 MT(60)를 위 SSD를 할 수 있다. VLR(50)은 MT(60)을 통해 UIM(62)에 난수 RAND를 전달하고, UIM(62)은 UIM(62)에 저장된 SSD 값과 RAND를 사용하여 일종 응답(AUTH)을 계산한다. AUTH에는 VLR(50)을 인터페이스 VLR(50)은 동일한 방법으로 독립적으로 계산되었던 AUTH와 같이 대해 리턴된 AUTH를 검사한다. 두 개의 AUTH 값이 동일하면, MT(60)가 위로 신뢰된다.

이 기법은 두 가지 점에 있어서 효과적이다. 첫째로, HLR(40)과 VLR(50) 사이의 장거리 시그널링 링크 (long-distance signaling link)를 통해 전달되는 데이터의 양이 매우 적고(128 비트 SSD), 하나의 고유한 인증을 전체 통화 세션에 대해 활용한다는 것이다. 둘째로, VLR(50)의 트라블러 제공을 방해한다. 왜냐하면 사용자를 인증할 수는 없다는 것입니다. 이는 RAND가 국부적으로 생성될 수 없고 HLR(40)에 의해 생성될 필요가 있기 때문에 가능한 것이다.

일호화 세션 키를 생성하기 위해, CAVE 알고리즘의 내부 상태는 인증 계산 후에도 유지된다. 이어서, 도 4에 도시된 바와 같이, CAVE의 인증 및 암호화 기능의 일부 키를 재생하여 몇 가지 레벨의 암호화 키가 제공된다.

국제 마동 이동 통신 - 2000 (IMT-2000) 표준을 개발하려는 노력과 무관은 세계 모든 곳에서의 경제 가입을 지원하고자 하는 가입자의 "전역 로밍(true mobility)"을 가능케 할 전역 적격 통신 시스템을 제공하는 것이다. 이 시스템은 무엇보다 위해서는 상이한 시스템으로부터의 가입자에 다른 시스템으로 "로밍"하는 것을 가능케 하는 다양한 시스템들(GSM, IS-41, PDC 등) 사이에 인터페이스가 제공되어야 한다. 현재로 그러한 "전역" 로밍이 보장되지 않다. 국제 등록 통신 협회(International Telecommunication Union : ITU)는 표준화된 네트워크 대 네트워크 인터페이스(network-to-network interface : NNI) 및 UIM-MT 인터페이스를 필요했을 것에 동일을 가능케 하고자 각 오퍼레이터 실체를 적절히 인증하는 메시지를 전달할 수 있어야 하는 표준을 개발하기 위해 노력하고 있다.

제 가능 UIM, 다중 모드 단말기는 개 마다의 몇몇 인터페이스 표준과 통신할 수 있는 단말기. 다중 모드 기반 UIM(장치를 통한 서비스 모델 정보를 소산하는 단말기를 포함하는 몇몇 유형의 전역 로밍이 가능해진다. 세 가지 문항 사항이 요동는 본 발명의 목적에 대하서는 동등하다. 하나의 네트워크부터 의 MMF가 상이한 인증 기법을 가진 네트워크를 방문하면, UIM은 국부 네트워크의 보안 구조(security architecture)를 통해 인증되어야 한다.

발명의 바람직한 실시 가능에 대해

본 방법은 상이한 인증 기법을 사용하는 네트워크 사이를 사용자들이 로밍함에 따라 사용자의 인증을 가능케 하는 단일 앤들 표년(AIF)을 제공함으로써 인증 문제를 해결한다. 또다 구체적으로, 하나의 네트워크로 서비스된 가능 트라블러를 사용하고 두 번째 네트워크로 로밍 바일 UIM(62)으로도 알려질 수 있는 필요 2 키 쿠를 사용하면 인증이 가능해진다.

인증 앤들 통신(AIF)은 각각의 통신 네트워크 게열(IS-41, GSM, PDC)의 인증 기법을 감출 조직한다. AIF는 홈 네트워크의 위치 앤티(authentication center : AC) 혹은 HLR 같은 네트워크로부 키 서버 위치할 수도 있다. 또한 AIF는 독립형 인터워킹 함수 통신(stand-alone interworking function : AIF)으로서 네트워크 내 로드 포어 위치할 수도 있다.

원격적으로 SSD 인증을 사용하는 네트워크의 사용자가 트라블러 기반 네트워크로 로밍할 때, AIF는 현재의 SSD값보다 리인증된 생성할 것이다. 트라블러 사용자가 SSD 네트워크로 로밍할 때, AIF는 트라블러로부터 SSD를 생성할 것이다.

본 발명의 AIF는 각각의 통신 네트워크 계열(GSM, IS-41, PDC) 내의 기존의 인증 구조를 유지시킨다. 추가적 통신 네트워크를 AIF, 네트워크로 에 네트워크 인터페이스(NNI), 사용자 단말 단말(UIM)에 부합하도록 만드는 변화에 간섭을 가중대고, 국제적 서스템에서 기존의 보안 레벨을 유지시킨다.

실시예 구현 및 작용

본 발명은 IMT-2000에서 전역 로밍자(roamer)를 인증하는 방법을 개시하고 있다. 인증 연동 펑션은 IS-41 MAP과 GSM MAP의 인증 구조를 통합하도록 제공된다. 특히, 인증 연동 펑션(AIF)은 두 개별(예를 들어, IS-41 및 GSM)의 인증 기법을 간을 중계한다. IS-41 사용자가 GSM 네트워크로 로밍할 때, AIF는 현재의 SSD로부터 트리플릿을 생성한다. GSM 사용자가 IS-41네트워크로 로밍할 때, AIF는 단일 트리플릿으로부터 SSD를 생성한다.

도 5는 기본 통신 시스템을 도시하고 있다. 단말기(102)는 인증 센터(106)와 접속되어 있는 네트워크(104)와 통신한다. 네트워크(104)는 네트워크 대 네트워크 인터페이스(NNI)(222)를 통해 제 2 네트워크(114)에 접속된다. 네트워크(114)는 단말기(116)와 인증 센터(112)에 접속된다.

도 6은 기본 이동 통신 시스템을 도시하고 있다.

도 6에 도시된 실시예에서, 홈 위치 레지스터(HLR)(302)과 방문 위치 레지스터(VLR)(304)는 제 1 네트워크(218)에 속하고 홈 위치 레지스터(HLR)(306)과 방문 위치 레지스터(VLR)(308)은 제 2 네트워크(220)에 속한다. 제 1 네트워크와 제 2 네트워크가 UIM(312)를 구비한 이동 단말기(310)의 사용자를 인증하는 데에 상이한 인증 기법을 사용할 때, 사용자를 네트워크 인증할 것인가에 대한 문제가 야기된다. 본 발명은 두 네트워크의 인증 기법을 간을 중계하는 인증 연동 펑션을 제공함으로써 이러한 문제를 해결한다. 본 발명에 개시된 인증 연동 펑션은 예컨대 IMT-2000에서 "전역" 로밍자를 인증하는 방법을 설명하고 있다. 이러한 인증 연동 펑션은 GSM 네트워크와 IS-41 네트워크 같이 상이한 인증 기법을 사용하는 두 네트워크의 인증 구조를 통합한다. 도 7 및 8은 GSM 네트워크와 IS-41 네트워크에서 사용된 네트워크 요소를 보다 상세히 설명하고 있다.

도 7은 GSM 네트워크인 제 1 네트워크(218)를 도시하고 있다. 이 네트워크는 홈 위치 레지스터(302), 방문 위치 레지스터(304), UIM(312)을 구비한 이동 단말기(310)를 포함하고 있다. 제 2 네트워크(220)는 IS-41 네트워크로서, 홈 위치 레지스터(306), 방문 위치 레지스터(308), UIM(312)을 구비한 이동 단말기(311)를 포함하고 있다. 도 7에 도시된 바와 같이, UIM(312)의 사용자가 다른 시스템, 예컨대 GSM 네트워크로 로밍할 때 인증 연동 펑션(314)이 사용된다.

도 8은 GSM 네트워크의 사용자가 IS-41네트워크로 로밍하는 반대의 경우를 도시하고 있다.

GSM 네트워크에서 로밍하는 IS-41 사용자

IS-41 사용자가 GSM 네트워크로 로밍할 때, AIF(314)는 SSD로부터 인증 트리플릿을 생성한다. 도 7에 도시된 바와 같이, HLR(306)은 현재의 저장된 SSD를 AIF(314)에 전달하고, AIF(314)는 SSD를 사용하여 트리플릿을 생성하고, 생성된 트리플릿은 VLR(304)에 전달된다. 따라서, VLR(304)은 MT(310)를 통해 UIM(312)에 RAND를 전달함으로써 UIM(312)을 인증한다. UIM(312)은 RAND 및 SSD를 이용해 SRES 및 K_c를 생성하여 SRES와 K_c를 MT(310)에 전달한다. MT(310)는 SRES를 VLR(304)에 전달하고, VLR(304)은 사용자를 인증하기 위해 이 SRES를 AIF(314)로부터 수신된 SRES와 비교한다. GSM VLR(304)은 등록 인지 메시지(registration notification message)(NNI REGNOT)를 이용해 네트워크 대 네트워크 인터페이스(NNI)(222)를 통해 트리플릿에 대한 리퀘스트를 AIF(314)에 전달한다. AIF(314)는 IS-41 HLR(306)로부터 사용자의 SSD를 검색하여 트리플릿(RAND, SRES, K_c)을 계산하는데 사용한다. 트리플릿은 응답 메시지 NNI REGNOT에 의해 GSM VLR(304)에 전달된다. AIF(314)는 트리플릿을 생성하는 데에 사용될 CAVE(혹은 IS-41 네트워크의 공통 암호 알고리즘(Common Cryptographic Algorithms : CCA) 내의 현재 인증 알고리즘)를 구비한다. 트리플릿 개념에 기인해, GSM 구조는 인증 알고리즘을 알 필요가 없으며, 이 알고리즘은 UIM(312) 및 IS-41 HLR(306)에만 존재한다. 달리 말하면, GSM VLR(304)은 CAVE를 구비할 필요가 없다.

챌린지 및 응답 파라미터의 크기는 IS-41 및 GSM 네트워크 사이에 차이가 있다. IS-41 SSD로부터 GSM 인증 쌍을 생성하기 위해 AIF(314)에서 크기 변환이 수행되는데, 특히, AIF(314)는 32 비트 RAND를 생성하고, CAVE 알고리즘을 사용하고 32 비트 RAND, 64 비트 SSD_A, 정해진 값, 인증 데이터 AUTH_DATA를 사용하여 18 비트 인증 응답 AUTHR을 계산한다. 또한 AIF(314)는 제로(zero) 혹은 더미(dummy) 값을 차후에 패딩함으로써 18 비트 AUTHR로부터 32 비트 SRES를 생성하고 32 비트 RAND로부터 128 비트 RAND를 생성한다.

통상적으로, IS-41 호 착신을 인증하는 동안에, 다이얼링된 디지트는 전역 챌린지가 리플레이(replay)되지 못하도록 보호하는 인증 데이터 AUTH_DATA로서 사용된다. 이는 GSM 네트워크 내에서는 이루어지지 않는데, 왜냐하면 다이얼링된 디지트가 알려지지 않을 때 트리플릿이 미리 계산되기 때문이다. 또한, 트리플릿은 단지 한 번만 사용되므로 리플레이 어택(attack)의 위험이 적다. 그러므로, SSD로부터 GSM 트리플릿을 생성할 때, AUTH_DATA는 고유의 챌린지 동안에서와 같이 국제 이동 가입자 정체(international mobile subscriber identity : IMSI)로 추정된다.

RAND 및 SRES 이후의 GSM 트리플릿의 세 번째 파라미터는 암산 키 K_c이다. 64 비트 루트 암호화(root encryption) 및 음성 프라이버시(voice privacy) 키 CMEA_KEY는 이러한 목적으로 사용된다. CMEA_KEY는 IS-41 TCAM 정의된 바와 같이 AIF(314)에 의해 아래와 같이 생성된다.

K_{c64} = CMEA_KEY$_{64}$ = CAVE(SSD_B, AUTH_STATE)

여기서, AUTH_STATE는 인증 응답이 계산된 후의 CAVE의 내부 레지스터의 상태를 나타낸다.

일단 K_c가 결정되면, 트리플릿은 완성되어 아래와 같은 NNI REGNOT 응답 메시지 내에서 AIF(314) 및 IS-41 HLR(306)을 경유해 GSM VLR(304)에 전달된다.

NNI REGNOT [$RAND_{32}$, $SRES_{32}$, K_{64}]

GSM VLR(304)이 트리플렛을 수신하면, UIM(312)이 CAVE를 사용하여 얻은 파라미터를 계산했다는 것을 제외하고는 IS-41 절차와 유사한 절차로 통상적 레귤레트 실행된다. 이 과정은 GSM 네트워크(216)에 대한 명령어나 ETS에 의해 제안된 표준에 따라 통상적으로 수행된다. 다음 메시지들이 생성되고 교환된다.

VLR(304) → HT(310) : RIL3-NN AUT-REQ [$RAND_{32}$].

HT(310) → UIM(312) : UIM AUTHREQ [$RAND_{32}$].

UIM(312) : $RAND_{32}$로부터 $RAND_A$를 추출함.

UIM(312) : $AUTHR_{32}$ = CAVE($RAND_A$, SSD_A, [정적], AUTH_DATA).

UIM(312) : $SRES_A$ = 좌측에 채로 놓은 한정 다미 비트가 패딩된 $AUTHR_{32}$.

UIM(312) : K_A = CMEA_KEY$_A$ = CAVE(SSD_B, AUTH_STATE).

UIM(312) → HT(310) : UIM AUTHRES [$SRES_{32}$, K_{64}].

HT(310) : 연산을 위해 K_A를 저장함.

HT(310) → VLR(304) : RIL3-NN AUT-RESP [$SRES_{32}$].

UIM(312)은 128 비트 인증 불한자($RAND_{128}$)를 파라미터로 사용하고 32 비트 인증 응답($SRES$) 및 64 비트 연산 키(K_A)를 제공한다.

IS-41 네트워크에서 모방하는 GSM 사용자

GSM 사용자가 IS-41 네트워크안에서 로밍할 때, 이동 단말기(311) 내의 UIM(312)과 IS-41 VLR(308) 사이에 공유 비밀 데이터(SSD)를 생성하는 것이 목적이다. 두 개에 달하 상세히 두사한 바와 같이, 두 개의 트리플렛은 HLR(302)로부터 AIF(314)로 전달되고, AIF(314)는 이들 트리플렛을 사용하여 SSD 업데이트 파라미터를 생성하여 VLR(308)에 전달한다. VLR(308)은 HT(311)을 통해 UIM(312)에 RANDSSDM_A와 RANDSSDM_B를 전송한다. UIM(312)은 RANDSSDM_A와 RANDSSDM_B를 사용하여 새로운 SSD 값으로 저장하는 K_A 및 K_B를 계산한다. 그에 따라, 각각의 시스템 액세스에 대하, VLR(308)은 IS-41에 정의된 인증 절차에 따라 SSD를 사용하여 HLR(302)에 상관없이 UIM(312)를 인증한다.

SSD 업데이트를 수행하기 위해 필요한 파라미터를 생성하는 데에 트리플렛을 사용하는 것이 GSM이다. 그 결과, IS-41 VLR(308)은 특정 GSM 사용자의 UIM(312)과 키(SSD)를 공유한다. 이에서, 각각의 시스템 액세스에 대해, 공유된 키는 UIM(312)과 IS-41 VLR(308) 사이에 공통되므로 일차적 인증 알고리즘과 함께 사용될 수 있다.

GSM 사용자로부터의 등록 시도가 검출되면, IS-41 VLR(308)은 AIF(314)에게 등록 인지(NNI REGNOT) 메시지를 전달한다. 이에서, AIF(314)은 GSM 사용자의 GSM HLR(302)로부터 두 개의 트리플렛을 요청한다. 이 과정은 GSM 네트워크(216)에 대해 명료하고 ETS에 의해 제안된 표준에 따라 이루어지며, 다음 메시지들이 HLR(302)에 의해 생성되고 AIF(314)와 교환된다.

HLR(302) : 128 비트 RANDGSM_A, RANDGSM_B를 생성함.

HLR(302) : K_A = A3(RANDGSM_A, K_i).

HLR(302) : K_B = A3(RANDGSM_B, K_i).

HLR(302) → AIF(314) : (RANDGSM_A, $SRES_A$, K_A), (RANDGSM_B, $SRES_B$, K_B).

AIF(314)는 등록 인지 메시지(NNI REGNOT)에 반응하여 SSD 업데이트 파라미터를 IS-41 VLR(308)에 반송하는데

AIF(314) : NewSSDInfo = (K_A, K_B),

AIF(314) → VLR(308) : NNI REGNOT [RANDGSM_A, RANDGSM_B, NewSSDInfo],

NewSSDInfo는 NewSSL_A = K_A와 NewSSD_B = K_B의 두 부분을 갖는다.

IS-41 VLR(308)은 파라미터 RANDU 및 AUTHU를 삽입한 후, (IS-41 AUTHDIR 메시지를 통해 : 이는 128 비트 RANDGSM 파라미터를 전달하기 위해 공유 안티테이스를 요구함을 명심하기 바람) HT(311)을 수신한 SSD 업데이트 절차를 수행한다. 이들 두 파라미터는 SSD 업데이트 중에 수행되는 고유의 절차상 동안에 사용된다. 이는 더 큰 (128 비트) RANDGSM 파라미터를 전달하도록 하기 위해 IS-41의 변화를 요구할 수 있음을 명심하기 바란다. (예에서, 다음의 메시지가 생성되고 교환된다.

VLR(308) : 한일 생한자 RANDU를 생성함,

VLR(308) : AUTHU = CAVE(RANDU, NewSSD_A, [정체]),

VLR(308) → HT(311) : SSD_UPDATE_GSM [RANDRSM_A, RANDGSM_B].

HT(311)는 (제안된 메시지 UIM UpdateSSD 1801A) UIM(312)에 파라미터를 전달하고, UIM(312)은 다음과

같이 새로운 SSD를 계산한다.

MT(311) → UIM(312) : UIM UpdateSSD [RANDSSN_A, RANDSSN_B].

UIM(312) : SSD_A = A8(RANDSSN_A, K).

UIM(312) : SSD_B = A8(RANDSSN_B, K).

UIM(312) : NewSSD = (SSD_A, SSD_B).

이제 공유 비밀 데이터는 IS-41 VLR(308)과 GSM UIM(312) 사이에 존재한다. 나머지 등록 주기에서 UIM(312)은 인증 파라미터를 계산하기 위해 K보다는 SSD_A를 사용한다. 유사하게, 비밀 SSD_B를 이용해 연산 키를 계산한다.

공통 인증 알고리즘

IS-41 VLR(308)과 UIM(312) 사이에 공유된 비밀 키가 존재한다. VLR(308)이 이동 단말기(311)와 함께 인증 및 세션 키 생성을 수행하기 위해서는 VLR(308)과 이동 단말기(311) 사이에 공유된 공통 암호화 알고리즘이 또한 필요하다. 이 알고리즘은 CAVE, A3/A8 혹은 임의의 인증 혹은 키 생성 알고리즘이 될 수 있을 것이다.

UIM(312)에만 변화가 생긴다면, CAVE는 알고리즘 A3과 함께 UIM(312)에 삽입된다. 원천적인 GSM 네트워크의 경우에는 A3이 루트 키 K와 함께 사용된다. IS-41 네트워크로 로밍할 때, CAVE는 전술한 바와 같이 SSD와 함께 사용된다.

IS-41 네트워크에만 변화가 생긴다면, 알고리즘 A3이 IS-41 네트워크에 포함된다. 여기서, IS-41 VLR(308)은 원천적인 IS-41 전화를 인증하기 위해 CAVE를 사용하고, GSM 로밍자를 인증하기 위해 A3을 사용할 수도 있다.

PDC와의 연동

일본 PDC 시그널링 MAP은 트리플렛 기반 구조와 매우 근사한 인증 기법을 사용한다. 로밍하는 사용자가 방문 네트워크에서 등록할 때, 홈 네트워크로부터 방문 네트워크로 전달되는 네트워크간 인증 정보 검색 메시지(Inter-Network Authentication Information Retrieval Message)에는 두 가지 버전(version)이 존재한다. 하나의 버전은 단순히 가입자 인증 키에 전달한다. 다른 버전은 난수, 조인 응답, 연산 키를 포함하는 인증 정보 리스트, 즉 인증 트리플렛을 전달한다. 그러므로, PDC는 IS-41과 유사한 SSD 기반 네트워크와 연동한다는 점에서 GSM과 동등하다. PDC 및 GSM 네트워크 모두가 트리플렛 기반 구조를 사용하기 때문에, 이들 네트워크 간의 접속이 비교적 용이하다. 그러나, GSM에서는 32 비트이고 PDC에서는 64 비트인 조인 응답 파라미터의 크기를 고려하면 부합되지 않는 문제가 존재한다. 한 해결은 PDC 사용자가 GSM 네트워크로 로밍할 때 PDC 시스템에 의해 리턴되는 32 비트의 응답을 단순히 무시하는 것이다. 이는 PDC 사용자가 익숙한 것보다 32 비트 낮은 보안을 제공한다.

보안

상기에서 논의한 인증 연동 개선은 각각의 시스템, 상기한 예에서의 GSM 및 IS-41 네트워크에 의해 통상 사용되고 있는 보안 체벨을 유지하도록 설계된다.

IS-41 사용자는 통상 32 비트 챌린지 및 18 비트 응답에 의해 인증된다. 이러한 파라미터들이 GSM 트리플렛 내의 더 큰 크기의 필드 내에 구비될 때 보안 레벨은 변하지 않는다.

GSM 사용자는 통상 128 비트 챌린지와 32 비트 응답에 의해 인증된다. IS-41 네트워크에서 로밍하고 있는 GSM 사용자의 인증은 더 적은 비트의 실보안(real security)(18 비트 AUTHR 및 32 비트 SRES)를 갖는 IS-41 크기 보안 파라미터에 의해 이루어진다. 그러나, 그들 자신의 시스템 내의 가정에서 GSM 사용자의 보안이 저하되지는 않는다. 또한, IS-41 네트워크에서 로밍할 때에 루트 키 K의 보안이 손상되지는 않는데, 그 이유는 a) SSD_A가 K 대신에 사용되고, b) IS-41 내의 챌린지/응답 쌍으로부터 루트 키로 되돌아가는 것은 어려움이 (키의 크기 - AUTHR의 크기인) 64-18 = 46 비트이기 때문이며, 이는 관찰된 각각의 챌린지-응답 쌍이 키스페이스(keyspace)를 64-32 = 32 비트로 축소시키는 GSM보다 더 안전하다.

IS-41 사용자에게 있어서 하나의 중요한 문제는 GSM 네트워크에서 로밍할 때 SSD 업데이트를 실행할 방법이 없다는 것이다. 현재의 SSD가 손상되거나 나빠지면, 사용자는 IS-41 네트워크로 다시 로밍하기까지 아무것도 할 수 없다. 또한, 이는 SSD가 유효하지 않기 때문에 GSM 네트워크에서 로밍하는 동안에 사용자는 가입(처음으로 네트워크에 액세스)할 수 없다는 것을 의미한다.

GSM 트리플렛은 통상 단일 호출에 대해서만 사용된다. 이러한 인증 연동 개선에서, GSM 사용자가 IS-41 네트워크로 로밍할 때, 단일 트리플렛은 많은 호출에서 존속하는 SSD_A로 변환된다.

그러나, SSD_A는 길이가 64 비트로 트리플렛 내의 32 비트 SRES의 두 배에 해당하는 보안 비트를 제공한다. 모든 것이 64 비트 루트 키 K로부터 생성되기 때문에 보안 레벨은 어쨌든 64 비트를 초과할 수는 없다. 반면에, 이제 인증은 SSD_A를 생성하기 위해 사용되는 A8에 의존한다. 이 보안 관계는 잘 알려져 있지 않다.

수출 규정(export regulation)을 고려하면, 본 출원서에 개시된 연산 키는 64 비트 수이다. 그러나, 정부 사안에 따르기 위해 언제든지 이를 줄일 수 있다. 사실상, UIM AUTHREQ 메시지는 연산 키의 크기를 지시하는 추가적 파라미터를 이용해 설계될 수 있다. 이러한 방식으로, 더 긴 키는 여전히 더 짧은 키 크기를

갖는 전력 수요처로 로밍될 수 있는 능력을 제공하면서 국소적으로 사용할 수 있다.

전술한 상세한 설명에 비록 IS-41 네트워크와 IS-41 네트워크 간의 로밍을 논의하고 있지만, 본 발명의 AIF(314)는 동일의 기술 플랫폼/플랫폼 상 인증 네트워크와 임의의 기본 키/플랫 간에 커 인증 네트워크 간의 통신을 촉진한다. 특히, 도 1에 도시한 바와 같이, 제 1 네트워크(210)는 인증 데이터 베이스(402)와 중계자(intermediary)(404)를 포함한다. 유사하게, 제 2 네트워크(220)는 인증 데이터 베이스(406)와 중계자(408)를 포함한다. 그러나, 도 2 내지 10에 도시한 바와 같이, 본 발명의 AIF(314)는 사용자로 하여금 제 1 네트워크(210)와 제 2 네트워크(220) 사이를 로밍&핸드록 한다. 또한, 도 2 내지 10의 특정형 네트워크 엔티티로서 AIF(314)를 도시하고 있지만, AIF(314)에 의해 수행되는 기능들은 도 2 내지 10의 HLR(302), VLR(304), HLR(305) 및 VLR(308) 중에서 하나 이상 혹은 도 11의 인증 데이터 베이스(402), 중계자(404), 인증 데이터 베이스(406) 혹은 중계자(408) 중에서 하나 이상에 구현될 수 있다.

특징적 요소

본 발명은 상이한 인증 기법을 사용하는 두 개의 통신 네트워크에서, SSD 인증을 사용하는 네트워크의 사용자가 트리플랙 기반 네트워크로 로밍할 때는 언제든 SSD로부터 트리플랙을 생성하고, 트리플랙 사용자가 SSD 네트워크로 로밍할 때는 트리플랙으로부터 SSD를 생성하는 인증 연동 절차 및 방법을 제공함으로써, 본 발명의 AIF는 각각의 동일 네트워크 계열 내의 기존의 인증 구조를 유지시키고, 두 개의 동신 네트워크를 AIF, 네트워크 대 네트워크 인터페이스(NNI), 사용자 정체 모듈(UIM)에 부합되도록 만들며, 각각의 시스템에서 기존의 보안 레벨을 유지시켜줌과도 사용자가 두 네트워크 간을 전역 로밍할 수 있도록 하는 장점이 있다

청구 범위 구성 요약

청구항 1

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자의 인증을 촉진하는 인증 연동 장선(authentification interoperability function)에 있어서,

상기 제 1 네트워크의 인증 데이터 베이스로부터 랜덤치/응답 쌍을 수신하고,

상기 랜덤치/응답 쌍으로부터 2차 커를 생성하며,

상기 제 1 네트워크로부터의 상기 사용자를 인증하기 위해 상기 제 2 네트워크의 중계자에 상기 2차 키를 전달하는

인증 연동 장선.

청구항 2

제 1 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 연동 장선.

청구항 3

제 1 항에 있어서,

상기 제 1 네트워크는 GSM(Global System for Mobiles) 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 중계자는 상기 IS-41 네트워크 내의 방문 위치 레지스터이고, 상기 인증 데이터 베이스는 상기 GSM 네트워크 내의 홈 위치 레지스터인 인증 연동 장선.

청구항 4

제 3 항에 있어서,

상기 인증 연동 장선은 상기 GSM 네트워크 내의 상기 홈 위치 레지스터와 함께 위치하는 인증 연동 장선.

청구항 5

제 3 항에 있어서,

상기 인증 연동 장선은 상기 IS-41 네트워크 내의 상기 방문 위치 레지스터와 함께 위치하는 인증 연동 장선.

청구항 6

제 3 항에 있어서,

상기 인증 연동 장치은 독립형 네트워크 엔티티(stand-alone network entity)인 인증 연동 장치.

청구항 7

제 1 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 형 인증 기법이고 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2개 키 인증 기법인 인증 연동 장치.

청구항 8

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자의 인증을 촉진하는 인증 연동 장치에 있어서,

상기 제 1 네트워크의 인증 데이터 베이스로부터 2차 키를 수신하고,

상기 2차 키로부터 챌린지/응답 쌍을 생성하며,

상기 제 1 네트워크로부터의 상기 사용자를 인증하기 위해 상기 제 2 네트워크 내의 중계자에 상기 챌린지/응답 쌍을 전달하는

인증 연동 장치.

청구항 9

제 8 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 연동 장치.

청구항 10

제 8 항에 있어서,

상기 제 1 네트워크는 IS-41 네트워크이고, 상기 제 2 네트워크는 GSM 네트워크이며, 상기 중계자는 상기 GSM 네트워크 내의 방문 위치 레지스터이고, 상기 인증 데이터 베이스는 상기 IS-41 네트워크 내의 홈 위치 레지스터인 인증 연동 장치.

청구항 11

제 10 항에 있어서,

상기 인증 연동 장치은 상기 IS-41 네트워크 내의 상기 홈 위치 레지스터와 함께 위치하는 인증 연동 장치.

청구항 12

제 10 항에 있어서,

상기 인증 연동 장치은 상기 GSM 네트워크 내의 상기 방문 위치 레지스터와 함께 위치하는 인증 연동 장치.

청구항 13

제 10 항에 있어서,

상기 인증 연동 장치은 독립형 네트워크 엔티티인 인증 연동 장치.

청구항 14

제 8 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기억 챌린지/응답 형 인증 기법인 인증 연동 장치.

청구항 15

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터

의 상기 사용자를 인증하는 방법에 있어서,

상기 제 1 네트워크의 인증 네이터 베이스로부터 챌린지/응답 쌍을 수신하는 단계와,

상기 챌린지/응답 쌍으로부터 키를 생성하는 단계와,

상기 키에 기초해서 상기 사용자를 인증하는 단계

를 포함하는 인증 방법.

청구항 16

제 15 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 인증 방법.

청구항 17

제 15 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 방법.

청구항 18

제 15 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 인증 데이터 베이스는 상기 GSM 네트워크 내의 홈 위치 레지스터인 인증 방법.

청구항 19

제 15 항에 있어서,

상기 제 1 네트워크의 인증 기법은 가역 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 인증 방법.

청구항 20

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자를 인증하는 방법에 있어서,

키로부터 챌린지/응답 쌍을 생성하는 단계와,

상기 제 1 네트워크 내의 중계자에 상기 챌린지/응답 쌍을 전송하는 단계와,

상기 챌린지/응답 쌍에 기초해서 상기 사용자를 인증하는 단계

를 포함하는 인증 방법.

청구항 21

제 20 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 인증 방법.

청구항 22

제 20 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 방법.

청구항 23

제 20 항에 있어서,

상기 제 1 네트워크는 IS-41 네트워크이고, 상기 제 2 네트워크는 GSM 네트워크이며, 상기 인증 데이터 베이스는 상기 IS-41 네트워크 내의 홈 위치 레지스터인 인증 방법.

22-9

청구항 24

제 20 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 인증 방법.

청구항 25

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자를 인증하는 인터페이스에 있어서,

상기 제 1 네트워크의 인증 데이터 베이스로부터 상기 제 2 네트워크 내의 중계자에 대로는 챌린지/응답 쌍을 구비하는 메시지를 포함하는 인터페이스.

청구항 26

제 25 항에 있어서,

상기 사용자는 이동 전화 가입자인 인터페이스.

청구항 27

제 25 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 인증 데이터 베이스는 상기 GSM 네트워크 내의 홈 위치 레지스터이고, 상기 중계자는 상기 IS-41 네트워크 내의 방문 위치 레지스터인 인터페이스.

청구항 28

제 25 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 인터페이스.

청구항 29

제 25 항에 있어서,

상기 제 1 네트워크는 IS-41 네트워크이고, 상기 제 2 네트워크는 GSM 네트워크이며, 상기 인증 데이터 베이스는 상기 IS-41 네트워크 내의 홈 위치 레지스터이고, 상기 중계자는 상기 GSM 네트워크 내의 방문 위치 레지스터인 인터페이스.

청구항 30

제 25 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법인 인터페이스.

청구항 31

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자를 인증하는 인터페이스에 있어서,

상기 제 1 네트워크 내의 중계자로부터 상기 사용자에 대로는 챌린지와 상기 사용자로부터 상기 제 1 네트워크 내의 상기 중계자에 이로는 응답을 구비하는 메시지를 포함하는 인터페이스.

청구항 32

제 31 항에 있어서,

상기 사용자는 이동 전화 가입자의 UIM(user identity module)이고 상기 중계자는 방문 위치 레지스터인 인터페이스.

청구항 33

제 32 항에 있어서,

상기 제 1 네트워크는 IS-41 네트워크이고, 상기 제 2 네트워크는 GSM 네트워크인 인터페이스.

청구항 34

제 32 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크인 인터페이스.

청구항 35

제 21 항에 있어서,

상기 메시지가 상기 제 1 네트워크 내의 상기 중계자로부터 상기 사용자에 의로는 난수(random number)를 더 포함하고, 상기 사용자가 상기 난수로부터 키를 생성할 수 있는 인터페이스.

청구항 36

제 35 항에 있어서,

상기 사용자는 이동 전화의 네트이고, 상기 중계자는 방문 위치 레지스터인 인터페이스.

청구항 37

제 35 항에 있어서,

상기 제 1 네트워크는 IS-41 네트워크이고, 상기 제 2 네트워크는 GSM 네트워크인 인터페이스.

청구항 38

제 35 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크인 인터페이스.

청구항 39

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자를 인증하는 중계자에 있어서,

상기 제 1 네트워크의 인증 데이터 베이스로부터 챌린지/응답 쌍을 수신하는 수신 요소와,

상기 챌린지/응답 쌍으로부터 키를 생성하는 생성 요소와,

상기 키에 기초해서 상기 사용자를 인증하는 인증 요소

를 포함하는 중계자.

청구항 40

제 39 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 중계자.

청구항 41

제 39 항에 있어서,

상기 사용자는 이동 전화 가입자인 중계자.

청구항 42

제 39 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 제 1 네트워크

내의 상기 인증 데이터 베이스는 상기 GSM 네트워크 내의 홈 위치 레지스터이고, 상기 중계자는 상기 IS-41 네트워크 내의 방문 위치 레지스터인 중계자.

청구항 43

제 39 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 중계자.

청구항 44

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자의 인증을 촉진하는 인증 데이터 베이스에 있어서,

키로부터 챌린지/응답 쌍을 생성하는 생성 요소와,

상기 챌린지/응답 쌍에 기초해서 상기 사용자를 인증하는 상기 제 1 네트워크 내의 중계자에 상기 챌린지/응답 쌍을 전송하는 전송 요소

를 포함하는 인증 데이터 베이스.

청구항 45

제 44 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 인증 데이터 베이스.

청구항 46

제 44 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 데이터 베이스.

청구항 47

제 44 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 제 1 네트워크 내의 상기 중계자는 상기 GSM 네트워크 내의 방문 위치 레지스터이고, 상기 인증 데이터 베이스는 상기 IS-41 네트워크 내의 홈 위치 레지스터인 인증 데이터 베이스.

청구항 48

제 44 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 인증 데이터 베이스.

청구항 49

사용자가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자를 인증하는 중계자에 있어서,

상기 제 2 네트워크의 인증 데이터 베이스로부터 챌린지/응답 쌍을 수신하되, 상기 챌린지/응답 쌍이 키로부터 생성된 수신 요소와,

상기 챌린지/응답 쌍에 기초해서 상기 사용자를 인증하는 인증 요소

를 포함하는 중계자.

청구항 50

제 49 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 중계자.

청구항 51

제 48 항에 있어서,

상기 사용자는 이동 전화 가입자인 중계자.

청구항 52

제 48 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 인증 데이터 베이스는 상기 IS-41 네트워크 내의 홈 위치 레지스터이고, 상기 중계자는 상기 GSM 네트워크 내의 방문 위치 레지스터인 중계자.

청구항 53

제 49 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 중계자.

청구항 54

사용지가 제 1 네트워크와 상이한 인증 기법을 갖는 제 2 네트워크에 있을 때, 상기 제 1 네트워크로부터의 상기 사용자의 인증을 촉진하는 인증 데이터 베이스에 있어서,

챌린지/응답 쌍으로부터 키를 생성하는 생성 요소와,

상기 키에 기초해서 상기 사용자를 인증하는 상기 제 2 네트워크 내의 중계자에 상기 키를 전송하는 전송 요소

를 포함하는 인증 데이터 베이스.

청구항 55

제 54 항에 있어서,

상기 키는 기본 키로부터 생성된 2차 키인 인증 데이터 베이스.

청구항 56

제 54 항에 있어서,

상기 사용자는 이동 전화 가입자인 인증 데이터 베이스.

청구항 57

제 54 항에 있어서,

상기 제 1 네트워크는 GSM 네트워크이고, 상기 제 2 네트워크는 IS-41 네트워크이며, 상기 중계자는 상기 IS-41 네트워크 내의 방문 위치 레지스터이고, 상기 인증 데이터 베이스는 상기 GSM 네트워크 내의 홈 위치 레지스터인 인증 데이터 베이스.

청구항 58

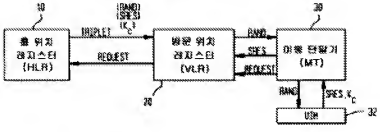
제 54 항에 있어서,

상기 제 1 네트워크의 인증 기법은 기억 챌린지/응답 쌍 인증 기법이고, 상기 제 2 네트워크의 인증 기법은 기본 키/공유 2차 키 인증 기법인 인증 데이터 베이스.

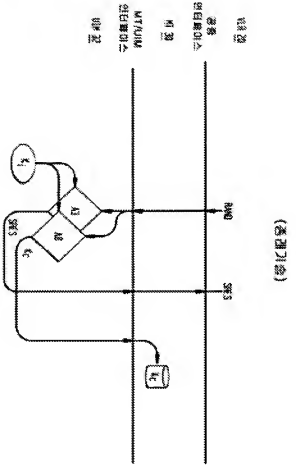
도면

도면1

(종래기술)

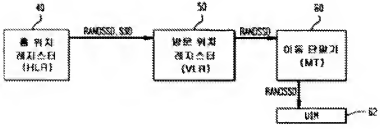


도면2



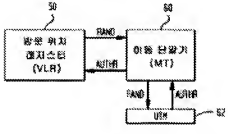
도면3a

(종래기술)

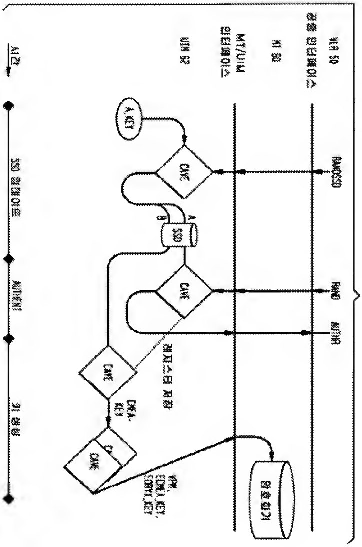


도면3b

(종래기술)

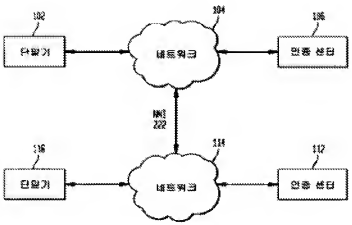


22-15

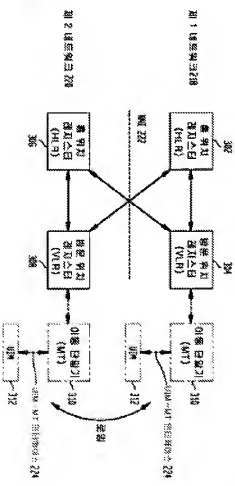

VLR 50
공중 인터페이스
MT/UIM
인터페이스
RANDSSD
RAND
AUTHR
CAVE
SSD
A_KEY
레지스터 저장
CMEA-
KEY
암호화기
시간
SSD 업데이트
AUTHENT
키 생성

(종래기술)

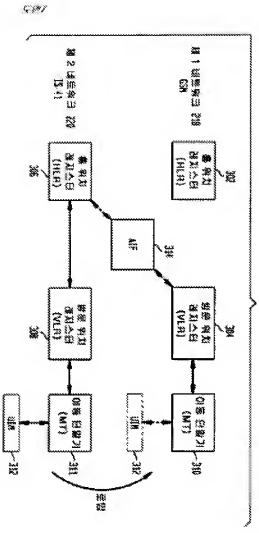
도면5


102
104
106
인터넷
인증 센터
222
112
114
116
인증 센터

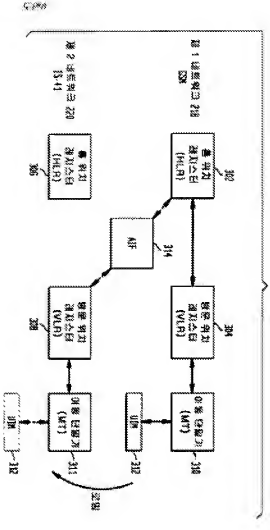
도면6


제 2 네트워크 220
제 1 네트워크 210
222
302
304
306
308
310
312
314
316
224
224

22-17


도면
제 1 네트워크 인터페이스 (NIF)
220
제 2 네트워크 인터페이스 (NIF)
210
송신 버퍼 (THER)
202
수신 버퍼 (THER)
206
AIF
334
송신 버퍼 (VLR)
204
수신 버퍼 (VLR)
208
이동 단말기 (MT)
201
이동 단말기 (MT)
203
SIM
232
SIM
234
교환

22-18


도면3
제 1 네트워크 인터페이스 325
제 2 네트워크 인터페이스 315
220
302
송/수신기 (제1RF)
306
송/수신기 (제2RF)
314
AIF
304
제1 모뎀 프로세서 (제1MP)
308
제2 모뎀 프로세서 (제2MP)
310
이동 단말기 (MT)
312
UIM
311
이동 단말기 (MT)
UIM
신호

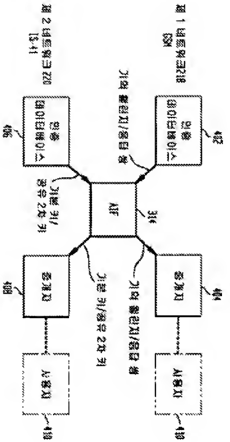
22-19

도면6
제 1 네트워크 218
SSN
제 2 네트워크 220
IS-41
MC 222
HLR 304
VLR 312
MS 310
ADF 314
AUTH
RAND
SRES
Kc
1. 트리플렛 및 RAND 요청
2. SSD 리 셰어링
3. SSD
4. 트리플렛 및 RAND, SRES, Kc
5. SRES
6. SRES
트리플렛은 RAND, SRES, Kc 를 포함
SRES=CAVE(RAND, SSD, A 타입 매개
Kc=CAVE(A KEY+CAVE(SSD, B
트리플렛은 RAND, SRES, Kc 를 포함
SRES=CAVE(RAND, SSD, A 타입 매개
Kc=CAVE(A KEY+CAVE(SSD, B

도면 22

제 1 네트워크 210
GSM
제 2 네트워크 220
IS-41
302
제어
2. 트리플렛 및 RAND 요청
3. 트리플렛 및
304
AUF
1. SID 인증 요청
306
VLR
4. SSD UPDATE
(RAND128, A_
RAND128, SSD)
5. SSD UPDATE 응답
(RAND128, A_
RAND128)
308
HE
6. RAND128, A_
RAND128, B
310
UIM
312
MIN
222

도면11


제 1 네트워크218
GSM
인증
데이터베이스
402
중계자
404
사용자
410
314
AIF
가역 챌린지/응답 쌍
가역 챌린지/응답 쌍
기본 키/공유 2차 키
기본 키/
공유 2차 키
제 2 네트워크 220
IS-41
인증
데이터베이스
406
중계자
408
사용자
410

22-22